Counterintelligence Quarterly

December 2005

Issue 10

From the desk of
Deputy Director, PPTAP, OCI
JOHN R. LEFTAULT

Happy New Year To All!

I am enthusiastic about my new position and arrive at an exciting, challenging, and opportune time to make a contribution to the DOE/NNSA Counterintelligence Program. My career background has been intelligence, security, and counterintelligence for more than 33 years. I spent 25 years in the U.S. Army, primarily serving overseas in the Pacific region. I have been with DOE and the CI Program since 2000. I joined OCI as an instructor, then as founding manager of the CI Training Academy (CITA) in Albuquerque, NM. Obviously, I continue to enjoy working in the CI field and look forward to sharing many career lessons learned in my new role.

The Plans, Policy, Training and Awareness Program (PPTAP) is in the midst of the OCI/ ODNCI Strategic Planning process, the National Intelligence Program (NIP) Budget Performance Management reporting, overall CN policy review, and the annual submissions of Individual Training Plans and CI Awareness Plans. These are all decisive ingredients of our CI program. I have also been fortunate to contribute in working groups with the new Office of the Director National Intelligence (ODNI) and the National Counterintelligence Executive (NCIX), now a part of ODNI. Many of the management and leadership tasks we must address, for our unique CI mission, are being determined from these offices. I encourage each of you to peruse *The National Intelligence Strategy of the United States of America* (October 2005) at http://www.dni.gov and *The National Counterintelligence Strategy of the United States of America* (March 2005) at *http://www.ncix.gov.*

I recognize that what we do best in our business is an art, not always a science. But I also believe it can be characterized and measured effectively to demonstrate how efficient we are with the resources given to us. This is one of the outcomes we hope to achieve in the strategic planning process now underway. Of course, it is also part of the NIP Budget Performance Management Report and data call that we provide to ODNI annually. The goals, objectives, performance indicators, and measurement targets being identified will help to determine what we are doing well, and where we need to improve. This is an absolutely essential activity to undertake at this time. Beginning in FY-2008, the ODNI in coordination with the respective Department Secretary can reallocate resources (read as money and staff) of those U.S. Intelligence Community (USIC) elements that are not effectively and efficiently utilized. Our CI Program is not in jeopardy, but we all need to remain in focus.

(Continued on Page 4)

Inside this Issue

Safe Passage Program

By:
Bonnie Hong, INL CI ISTP TE ,
Dr. Bruce L. Albright, INL, CI Analyst,
Jodi Hansen, INL, CI Specialist

Scientists at the U.S. Department of Energy's (DOE) Idaho National Laboratory (INL) developed the Change Detection System (CDS) technology that highlights slight differences between digital images. The CDS program aligns images, to within a fraction of a pixel, from hand-held or otherwise imprecise cameras. The alignment compensates for differences in camera angle, height, zoom or other distractions. Using identical reference points in each view, CDS maximizes the similarities between them. Then, by flipping back and forth between the two like an animation, previously unnoticeable differences emerge from the background. CDS can be operated from any standard desktop or portable computer, plus it works from almost any digitized image format. Initially developed for a variety of national security users, the system could potentially be used whenever small yet important changes occur. Use of the CDS technology in security, the medical profession or in manufacturing industries is nearly unlimited. The CDS technology was a 2003 winner of R&D magazine's top 100 technologies competition.

In the past, the best technology available for comparing images has been the flip-flop technique, which capitalizes on the visual reflex that draws our eyes toward motion. Rapidly alternating between two similar digital images on a screen creates an animation effect where identical elements seem stationary and differences appear as movement. However, the flip-flop approach requires that both pictures be shot from the exact same position using a mounted camera. Since stationary cameras are impractical in many cases, flip-flop comparisons are often impossible.

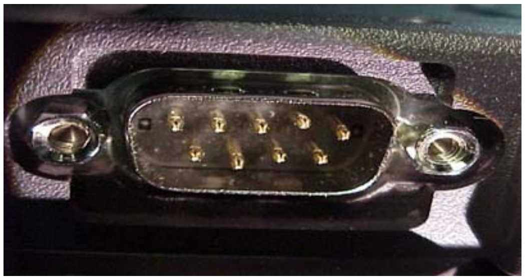
(Continued on Page 2)

Safe Passage (Continued from Page 1)

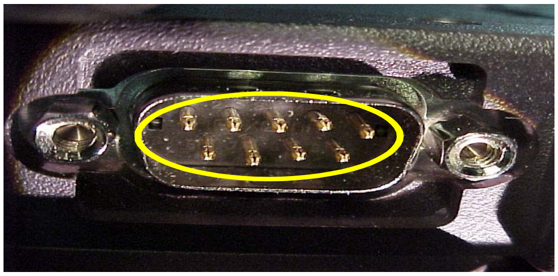
CDS technology combines the strengths of rote computer analysis with the powerful human reflex elicited by the flip-flop technique. Potential applications for this technology include surveillance (detect whether doors have been opened or cars have been moved), forensics (compare tire prints or fingerprints), national security (reveal tampering with container locks and seals), home security (divulge whether drawers or rooms were disturbed), field research (monitor environmental changes), and medical applications (change in size of tumors/growths).

One of the applications this technology has proven useful is as a tool within the laptop inspection program used by several DOE sites. INL Counterintelligence (CI) incorporated this technology into a package that includes the software, a scanner, and a user's manual called the "Safe Passage Program" (SPP).

The SPP allows sites across the DOE complex to baseline the physical exterior of laptops taken on travel to foreign countries. Digital images are taken of all sides of the laptop. Upon return from travel, digital images are taken and comparisons of all the images are made. The SPP software quickly compares two similar images to determine if the laptop was tampered with (i.e. battery removed, pins moved, etc.). INL CI collaborated with the DOE Cyber Forensic Laboratory (CFL) in Elkridge, MD, to allow for extensive analysis of DOE laptops that have indications of compromise. Compare the two pin pictures below, the yellow highlighting shows the differences that SPP detected in the two digital images. Notice how the pins have been moved.

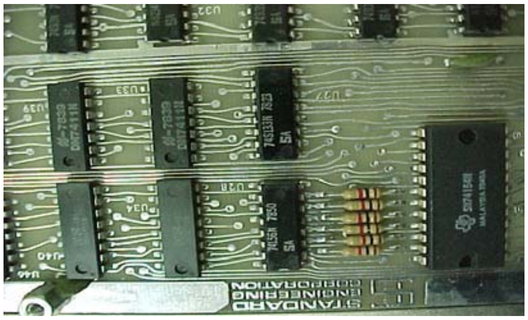


Before

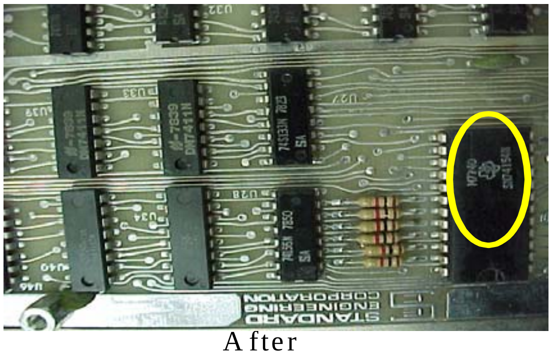


After

A recommendation is made to each site to have the laptop hard drive image ghosted before and after a trip in addition to SPP. In the event, there is an indication of physical tampering. The laptop, SPP images (both before and after), and the hard drive software images can be packed up and sent to CFL for extensive analysis. The hard drive software images will allow detection of malicious code, file modification, or data manipulation. The hard drive image may be sent along with the digital images of the physical exterior to see if malicious code was installed or if any of the files were modified. Compare the two circuit board pictures below, the yellow highlighting shows the differences that SPP detected in the two digital images. Notice that the chip has been changed.



Before



After

SPP has proven to be very useful in counterintelligence work. Additional DOE sites are requesting the SPP. For additional information about the Safe Passage Program, contact Allen Lundeen at Allen.Lundeen@inl.gov or call him at (208) 526-2341.

Counterintelligence Press Highlights

By Gary Chidester—HQ

Three Charged With Acting As Foreign Agents For the People's Republic of China. According to a Department of Justice News Release of November 15, 2005, a federal grand jury in Los Angeles indicted three Chinese natives on charges of acting as agents of a foreign government without prior notification to the Attorney General of the US.

The indictment against the three defendants supersedes a criminal complaint filed on October 28 that accused them of theft of government property. The one-count indictment charges:

- Chi Mak, 65, a naturalized US citizen;
- Chi Mak's brother, Tai Wang Mak, 56, who is residing in the US as permanent resident alien; and Chi Mak's wife, Rebecca Laiwah Chiu, 62.

The three defendants, along with a fourth who is not charged in the indictment, were arrested on the night of October 28 pursuant to a criminal complaint. Following their arrests, Chi Mak and his brother were ordered detained, or held without bond. Chiu was released last week after posting a $300,000 bond.

According to the affidavit in support of the criminal complaint, Chi Mak was an engineer for a company named Power Paragon. Allegedly, Chi Mak transferred data relating to a sensitive government project to his home, where his wife assisted him in copying the information onto CDs. Chi Mak delivered the CDs to his brother, who encrypted the information and made arrangements to transport it to the People's Republic of China. Tai Mak allegedly planned to travel to the PRC to deliver the information.

The charge of failing to register as a foreign agent carries a maximum possible penalty of 10 years in federal prison. The investigation was conducted by the Federal Bureau of Investigation in conjunction with the Naval Criminal Investigative Service.

Protecting Sensitive Information in the Midst of Globalization

By Anne Reed — RL-OCI

Frequently asked questions by our employees prompted this article. They are concerned about the effects of globalization and how it's affecting the Department of Energy's (DOE) research and development, and the U.S. market as a catalyst of the world's economy. This is a gray area and we have to ask ourselves where is the line between a globalized economy and the compromise of U.S. proprietary and unclassified sensitive information? Foreign nationals have increased access to this information within the U.S. through official foreign visits to DOE and military facilities, as students attending our academic institutions, and through employment at U.S. firms. Globalization is also increasing access to U.S. technologies outside our borders.

In September 2005 Michelle Van Cleave from the Office of National Counterintelligence Executive (ONCIX) spoke before the House Judiciary Subcommittee on Immigration, Border Security & Claims during a hearing on Sources and Methods of Foreign Nationals Engaged in Economic and Military Espionage. She addressed the difficulty of protecting technologies developed or acquired by U.S. companies from the fusion of foreign and U.S. firms due to globalization. Many U.S. companies are taking their operations overseas. Proprietary and/or sensitive technologies needed to operate overseas have a great potential for being compromised. Foreign investment in U.S. firms has increased over the past few years. Van Cleave reported, "In 2004 alone, according to the Department of Commerce, foreign investment in the U.S. amounted to more than $100 billion."

Recent foreign acquisitions of U.S. high tech firms include Singapore Technologies' purchase of Global Crossing, a fiber optic network provider, and China's computer firm Lenovo's purchase of IBM's personal computer business.

There is growing concern regarding economic and industrial espionage involving government and private industry's proprietary and sensitive information. Providing awareness information to our employees on these issues is essential. The Tech Transfer Notes developed and distributed from Lawrence Livermore National Laboratory (LLNL) is a great resource. Each month it documents news articles involving economic and industrial espionage occurring within the U.S and involving American firms.

Many countries consider U.S. technology essential to their economic and military growth and their creativeness to acquire such technology is endless. We are well aware of the easiest method, which is simply asking for the information via unsolicited emails or personal contact at conferences and seminars. Van Cleve notes we still face significant gaps in understanding foreign collection methods, and a few less acknowledged techniques are listed below:

- "Having dedicated programs whose primary task is technology acquisition. These programs often involve the use of front companies, which operate surreptitiously.
- 'Laundry lists' of targeted technologies and specific strategies for acquisition. Where an entire system cannot be acquired, there may be attempts to steal component parts.
- Arrangements to share technology that has been both legally and illegally acquired with other countries' intelligence and security services, even when the sharing of that technology is itself illegal."

Globalization is economically beneficial to the U.S., but it makes our job of protecting our proprietary and unclassified sensitive information that much more difficult. Using available resources to convey our awareness messages about less obvious collection techniques is important to ensure our employees stay informed. Pointing out the reality of front companies, foreign countries' needs for specific, but hard to acquire component parts, and collection techniques used by foreign adversaries will help our employees stay aware if or when these situations occur. After all, knowledge is power. .. **know** who you are dealing with!

Leadership Message

Continued From Page 1

The OCI/ODNCI staff, across the complex, must also have the professional development training opportunities available to further their knowledge, skills, and abilities to succeed. I will be working closely with the ODNI/NCIX staff to increase the number of training allotment opportunities in external USIC courses for our staff. Each of you, as key members of the OCI/ODNCI staff, should plan to attend at least one CI-related professional development course opportunity annually. This is one of the performance indicators for our NIP Budget Performance Management Report to ODNI and Congress. There are many different course options available, both internally and externally, to us in DOE/NNSA. PPTAP will continue to announce these opportunities as they become available. Keep your Individual Training Plan up-to-date and submit course-specific training nominations as requested. We also want your feedback on the value of such training in relation to your position, so send us an email when you complete the course.

I also continue to trust powerfully in presenting espionage or terrorism awareness education to all our employees as a deterrent to foreign directed or sponsored collection activities, and as a means to reinforce employee reporting of activities or behavior of CI concern. I personally know the CITA and each SCIO work very hard to do this for the entire Department. I strongly encourage each SCIO to use the CITA instructional staff and their resources to help design, develop, and deliver highly tailored awareness presentations for employees involved in high risk programs, for those attending meetings/conferences involving sensitive country representation, for those on recurring foreign travel, and for those involved in Foreign Visits & Assignments. This would be in addition to your CI Briefing program.

In closing, I am very proud to be part of such a quality group of CI professionals serving across the DOE/NNSA complex. For those of you I haven't met, I hope to do so as time goes on. I view my primary role as being a facilitator and instrument to serve your needs, and that of the entire CI program, in planning, policy matters, professional development training, and CI/CT awareness education for all DOE/NNSA employees, federal or contractor. Should you have any ideas to share, please pass them on to me.

Awareness Program Gizmos and Gadgets

By Deanna Austin—HQ

Flip the top, click the button and close the case. No switching ON is required.

This inconspicuous, "Zippo"-looking lighter actually contains a digital camera capable of capturing and holding up to 300 highly-detailed images built with incredibly small file sizes. Special technology even allows clear images in fluorescent light without using a flash.

This camera can also be set in the surveillance mode that will automatically capture images at pre-set time intervals for as many as 19 days. Video clips with sound – up to 30 seconds – allows instant data capture and an additional 12 minutes of sound recording can allow dictation to fill in the details. With 8MB of total storage, important data can be moved between computers utilizing this camera as a portable hard disc drive and uses USB Plug-n-Play for easy use.

ARTICLE SUBMISSIONS AND READER FEEDBACK WELCOME

Counterintelligence Quarterly: Reporting on the nexus between quality science, technology and counterintelligence

Published by:
U.S. Department of Energy
Office of Counterintelligence and
Office of Defense Nuclear
Counterintelligence
1000 Independence Avenue, SW
Washington, DC 20585

Managing Editor:
Clarenda Moore McKnight
202 586-1756 (Ph)
202 586-0551 (Fax)
clarenda.mcknight@cn.doe.gov

LOCAL COUNTERINTELLIGENCE OFFICE CONTACT INFORMATION

Office of Counterintelligence Richland Regional Office

Contact us: By Email:
^OCINWREGION
OCINWREGION@RL.GOV

By Telephone: 373-1865

Visit our website at:
http://www.hanford.gov/oci/index.cfm